⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平1－219982

⑤1Int. Cl.⁴	識別記号	庁内整理番号	㊸公開　平成1年(1989)9月1日
G 06 K 19/00		P－6711－5B	
B 42 D 15/02	331	J－8302－2C	

審査請求　未請求　請求項の数 4　（全5頁）

㊹発明の名称　ＩＣカード

㉑特　願　昭63－46304
㉒出　願　昭63(1988)2月29日

㉒発明者　品川　徹　大阪府茨木市丑寅1丁目1番88号　日立マクセル株式会社内
㉑出願人　日立マクセル株式会社　大阪府茨木市丑寅1丁目1番88号
㉔代理人　弁理士　梶山　信是　外1名

明　細　書

1.発明の名称　ＩＣカード

2.特許請求の範囲

(1) プロセッサと、このプロセッサのシステムプログラムを格納する第1の不揮発性メモリと、アプリケーションプログラムを格納する書換え可能な第2の不揮発性メモリと、各種の処理データを記憶する書換え可能な不揮発性メモリ又は揮発性メモリからなる第3のメモリとを有し、外部装置との間でデータの授受を行うＩＣカードにおいて、前記プロセッサのアクセスアドレスがアクセスしてはいけないアドレス値又はアドレス範囲であるか否かを判定してアクセス禁止信号を発生する禁止アドレス判定手段と、前記アプリケーションプログラムが起動されたとき又は前記アプリケーションプログラムが実行されているときにそのことを示す動作信号を発生する動作信号発生手段と、この動作信号があるときに、前記アクセス禁止信号に応じて前記プロセッサが第2の不揮発性メモリ又は第3のメモリをアクセスすることを禁止するアクセス禁止手段とを備えることを特徴とするＩＣカード。

(2) 禁止アドレス判定手段は、アプリケーションプログラムが実行されたときにアクセスしてはいけないアドレス値又はアドレス範囲を第1，第2及び第3のメモリのいずれかに有していることを特徴とする請求項1記載のＩＣカード。

(3) 禁止アドレス判定手段は、アプリケーションプログラムが実行されたときにアクセスを許可されるアドレス値又はアドレス範囲を第1，第2及び第3のメモリのいずれかに有していることを特徴とする請求項1記載のＩＣカード。

(4) 第3のメモリは書換え可能な不揮発性メモリであって、第1，第2及び第3の不揮発性メモリの少なくとも2つは、書換え可能な1つの不揮発性メモリの分割されたエリアに割り当てられていることを特徴とする請求項1乃至請求項3のうちのいずれか1項記載のＩＣカード。

3.発明の詳細な説明

［産業上の利用分野］

この発明は、ＩＣカードに関し、詳しくは、ＩＣカード内部に格納されたアプリケーションプログラムの暴走等によってシステム制御情報等が破壊されてしまうことがないようなＩＣカードの改良に関する。

［従来の技術］

ＩＣカードは、通常、内部にマイクロプロセッサとメモリ、そして外部装置との間でデータの授受を行うためのインタフェース等とを内蔵していて、例えば、外部装置の１つであるホストコンピュータとか、ＩＣカードリーダ・ライタに装着されて使用され、外部装置から発信されたコマンド群をＩＣカードの内部制御プログラムが解読し、メモリに記憶された動作プログラムに従って、そのメモリのアクセス、例えばデータの書込み、読出し及び消去等を実行し、その結果をコマンドに対するレスポンスとして外部記憶装置に返答するシーケンスに従って外部装置との間でデータの授受を行う。

このようなＩＣカードは、従来、マイクロプロセッサの処理プログラムがマスクＲＯＭ内に格納されていて、その内容を変更することはできなかったが、例えば、特開昭６１－２１１７８８号公報に示されているように、電気的消去可能な不揮発性メモリ（ＥＥＰＲＯＭ）をプログラム用メモリとして用いることにより、プログラムの内容を変更することが可能である。

［解決しようとする課題］

このようなＥＥＰＲＯＭを内蔵していて、そのプログラムの書換えができるＩＣカードは、一般に、カード内の制御を行うシステムプログラムが書換え不可能なマスクＲＯＭに格納されていて、用途によって決定されるアプリケーションプログラムがＥＥＰＲＯＭに格納されている。

したがって、アプリケーションプログラム上からマイクロプロセッサが管理するメモリ領域の全てをアクセスすることが可能である。そこで、システムプログラムが使用しているメモリ領域や、ハードウエアの設定を行うレジスタ類などの領域をアプリケーションプログラムがその暴走等によりアクセスした場合にそこにあるデータが破壊されてしまい、ＩＣカードが動作不能となる危険性がある。

この発明は、従来のＩＣカードがシステム制御情報等の破壊によって動作不能というような危険性をなくし、以て信頼性の高いＩＣカードを提供することを目的とする。

［課題を解決しようとする手段］

このような目的を達成するためのこの発明のＩＣカードの構成は、プロセッサと、このプロセッサのシステムプログラムを格納する第１の不揮発性メモリと、アプリケーションプログラムを格納する書換え可能な第２の不揮発性メモリと、各種の処理データを記憶する書換え可能な不揮発性メモリ又は揮発性メモリからなる第３のメモリとを有し、外部装置との間でデータの授受を行うＩＣカードにおいて、プロセッサのアクセスアドレスがアクセスしてはいけないアドレス値又はアドレス範囲であるか否かを判定してアクセス禁止信号を発生する禁止アドレス判定手段と、アプリケーションプログラムが起動されたとき又はアプリケーションプログラムが実行されているときにそのことを示す動作信号を発生する動作信号発生手段と、この動作信号があるときに、アクセス禁止信号に応じてプロセッサが第２の不揮発性メモリ又は第３のメモリをアクセスすることを禁止するアクセス禁止手段とを備えるものである。

［作用］

このように、アプリケーションプログラムからのメモリアクセスを禁止するために、アプリケーションプログラムが動作していることを示す信号を発生するアプリケーションプログラム動作信号発生部と、例えば、アクセスを禁止したいアドレス又はアクセスを許可するアドレスを保持していて、禁止アドレスがアクセスされた場合に、アクセス禁止信号を発生する禁止アドレス判定部とを設けて、アプリケーションプログラム動作信号と、アクセス禁止信号とからアクセス禁止手段によりアプリケーションプログラムの起動又はその実行によって禁止アドレスがアクセスされないように

プロセッサのアクセスを禁止するようにしているので、たとえアプリケーションプログラムが暴走したとしても、システム制御情報を記憶するレジスタとかそれを記憶するＲＡＭ等のアドレスのアクセスを禁止できる。

その結果、システム制御情報等が破壊されないで済み、ＩＣカードの動作停止等を防止でき、信頼性の高いＩＣカードを発行できる。

［実施例］

以下、この発明の一実施例について図面を参照して詳細に説明する。

第１図は、この発明によるＩＣカードの一実施例を示すブロック図、第２図は、その情報記憶部のメモリマップである。

第１図において、１０は、ＩＣカードリーダ・ライタ（又はホストコンピュータ）に装着されて、ＩＣカードリーダ・ライタとの間でデータの授受を行うＩＣカードであって、１は、その情報処理部（マイクロプロセッサ，ＭＰＵ）である。そして、このＭＰＵ１の制御プログラムとか基本的処理プログラムや動作プログラムが情報記憶部４に記憶されている。３は、その信号入出力部であり、ＭＰＵ１はこの信号入出力部３を介して外部装置との間でデータの授受を行う。

通常の動作においては、ＭＰＵ１が情報記憶部４のＥＥＰＲＯＭ等に記憶されたプログラムに従って、所定の処理を実行し、情報記憶部４のＲＡＭに外部装置から転送されたデータとか、読出しデータ、結果データ等を一時的に記憶し、ＩＣカードリーダ・ライタ等の外部装置との間でデータの授受が行われる。

ＭＰＵ１は、その機能ブロックとして、ここでは、演算処理部２、禁止アドレス判定部５、アクセス管理部６、そしてアプリケーションプログラム動作信号発生部７とにより構成されている。なお、これら構成要素の一部或いは全部は、ハードウエアとして回路により実現されても、また、情報記憶部４に記憶された対応する各処理プログラムを実行することで実現されてもよい。さらにこれらは、ハードウエアとソフトウエアとの組合せで実現されてもよい。

ここで、禁止アドレス判定部５は、情報記憶部４のうちのアプリケーションプログラム４２がアクセスできない範囲の上限及び下限のアドレスを複数保持していて、演算処理部２から発生するアドレス信号を得て、そのアドレスが前記上限アドレス及び下限アドレスの範囲内あるか否かを判定し、その範囲にあるときにはアクセス禁止信号８をアクセス管理部６に送出する。なお、上限アドレス値及び下限アドレス値の保持は、アプリケーションプログラム４２の情報記憶部４への格納とともに情報記憶部４の所定の領域に記憶されることで行われ、その設定、変更が可能である。

アクセス管理部６は、演算処理部２から発生するアドレス信号を受けて、アクセスを禁止すべきでないときには、それを情報記憶部４へと出力し、アクセスを禁止すべきときには、その出力を停止させる。ここで、アクセスが禁止される状態としては、アプリケーションプログラム動作信号発生部７からアプリケーションプログラム動作中であることを示す信号を受けているとき又は受けたとき、すなわち、アプリケーションプログラム動作信号９を受けているとき又は受けたときに、前記禁止アドレス判定部５から送出されるアクセス禁止信号８に応じて行われ、ことのき演算処理部２から情報記憶部４へのアドレス信号の送出が停止される。さらに、このとき同時に、アクセス管理部６は、演算処理部２へ異常アクセス信号１５を出力する。

アプリケーションプログラム動作信号発生部７は、システムプログラム４１によってアプリケーションプログラム４２が起動されると、アプリケーションプログラム動作信号９を発生して、それをアクセス管理部６へと送出する。

情報記憶部４は、ＭＰＵ１がアクセスするアドレス空間に割り当てられた記憶部であって、第２図に示すように、この情報記憶部４の所有するアドレス空間には、内部レジスタ１１と、ＲＡＭ１２、アプリケーションプログラムエリア１３、そしてシステムプログラムエリア１４とがそれぞれ

割り当てられていて、アプリケーションエリア１３にはＥＥＰＲＯＭが配置され、そこに書込まれるデータとかプログラムは書換えが可能となっている。一方、システムプログラムエリア１４には、マスクＲＯＭが配置され、そこに書込まれたデータ或いはプログラムは書換えが不可能となっている。

このような記憶部のアドレス空間割り当てに対して、最初は、システムプログラムエリア１４にシステムプログラム４１が格納されており、アプリケーションプログラムは、未だ格納されていない状態にある。この状態でＭＰＵ１は、システムプログラム４１を用いて、外部装置よりアプリケーションプログラム４２を信号入出力部３を介して受けてこれをアプリケーションプログラムエリア１３に格納する処理を行い、用途に応じて選択されたアプリケーションプログラム４２が搭載される。このとき、その用途に応じたＩＣカードが作り上げられる。

その後、アプリケーションプログラム４２が起動されて動作を始め、所定の用途に適合した動作が行われるが、アプリケーションプログラム４２にバグ等があったり、電源電圧の変動等により誤動作をすると、情報記憶部４の中で本来はアクセスする必要のないアドレス部分がアクセスしてしまうことが生じる。

情報記憶部４の中には、第２図に示すように、ＩＣカード１０内の各部の制御のための内部レジスタ１１、処理を行う際の作業領域等として用いるＲＡＭ１２が含まれているので、アプリケーションプログラム４２の実行によってＭＰＵ１が故意に或いはその動作不良等によって内部レジスタ１１或いはＲＡＭ１２の内容を書換えてしまうと、システムプログラム４１によって設定された状態が変化してしまう。そこで、システムプログラム４１の動作が異常となって、ＩＣカード１０が動作不能に陥る可能性がある。

このようなときにこの実施例では、アクセス管理部６により情報記憶部４のアクセスが次の手順で禁止され、前記の書換えが行われることはない。

すなわち、禁止アドレス判定部５にはアクセスを禁止したいアドレスが保持（登録）されているので、前記の場合には、まず、アクセス禁止信号８が発生する。一方、システムプログラム４１によってアプリケーションプログラム４２が起動されると、アプリケーションプログラム動作信号発生部７からアプリケーションプログラム動作信号９が発生している。そこで、アクセス管理部６は、アプリケーションプログラム動作信号９とアクセス禁止信号８とから、アプリケーションプログラム４２の実行によりアクセス管理部６へのアクセスが行われたことを検出し、この時点で情報記憶部４へのアクセスを行わず、処理部２へ異常アクセス信号１５を発生する。

演算処理部２が異常アクセス信号１５を受けたときには、アプリケーションプログラム４２の実行を停止して、その旨の信号を外部装置等へと送出する処理をするか、特定の記憶領域にその意味を示すフラグを立てる。

以上のように、アクセスが禁止されるべきアドレスを単に禁止アドレス判定部５に設定しておけば、その領域のアクセスが行われず、システム制御情報等が破壊されないで済む。なお、禁止アドレス判定部５のアクセス禁止範囲又は禁止アドレスを示すアドレスの上限値及び下限値又はあるアドレス値は書換えられてはいけないので、これらは、アプリケーションプログラム４２からアクセス不可能アドレス空間に割り当てられる。これらのアドレス値は、ＲＡＭ等を用いて任意に設定、変更可能としてもよいし、書込み可能な不揮発性メモリ等を用いて設定のみ可能で変更不可能なものとしてもよい。また、これは、ＩＣの製造時等に設定し、以後設定、変更不可能としてもよい。なお、禁止範囲は上限値及び下限値として示されるアドレス範囲だけでなく、１つのアドレス一点であってもよく、このような禁止アドレスを複数記憶しておいても、１つだけ記憶しておいてもよい。その数は問うものではない。

実施例では、アクセスが禁止されるアドレスに対してアクセスされるアドレスを判定して禁止信

号を発生しているが、アクセスが許可されているアドレスを記憶しておき、アクセスされるアドレスが許可されているアドレスの範囲か否かを判定してそれを越えているときにアクセス禁止信号を発生してもよい。

実施例における演算処理部２、禁止アドレス判定部５、アクセス管理部６、そしてアプリケーションプログラム動作信号発生部７をソフトウエアで実現するときの信号の送出は、例えば、メモリの割り当てられた特定の領域にフラグを立てることで行い、信号を受ける方がその割り当て領域にフラグが立てられているか否かを判定することによってもよい。

［発明の効果］

以上説明したように、この発明にあっては、アプリケーションプログラムからのメモリアクセスを禁止するために、アプリケーションプログラムが動作していることを示す信号を発生するアプリケーションプログラム動作信号発生部と、例えば、アクセスを禁止したいアドレス又はアクセスを許可するアドレスを保持していて、禁止アドレスがアクセスされた場合に、アクセス禁止信号を発生する禁止アドレス判定部とを設けて、アプリケーションプログラム動作信号と、アクセス禁止信号とからアクセス禁止手段によりアプリケーションプログラムの起動又はその実行によって禁止アドレスがアクセスされないようにプロセッサのアクセスを禁止するようにしているので、たとえアプリケーションプログラムが暴走したとしても、システム制御情報を記憶するレジスタとかそれを記憶するＲＡＭ等のアドレスのアクセスを禁止できる。

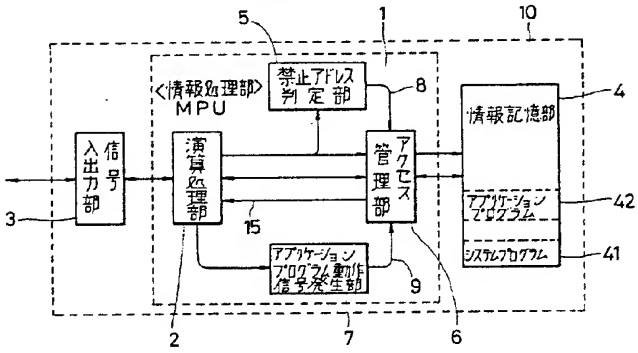
その結果、システム制御情報等が破壊されないで済み、ＩＣカードの動作停止等を防止でき、信頼性の高いＩＣカードを発行できる。

4.図面の簡単な説明

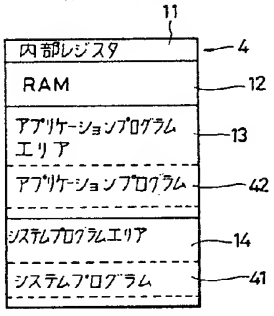
第１図は本発明によるＩＣカードの一実施例を示すブロック図、第２図は、その情報記憶部のメモリマップを示す説明図である。

１…情報処理部（ＭＰＵ）、２…演算処理部、３…信号入出力部、４…情報記憶部、５…禁止アドレス判定部、６…アクセス管理部、７…アプリケーションプログラム動作信号発生部、８…アクセス禁止信号、９…アプリケーションプログラム動作信号、１０…ＩＣカード、１１…内部レジスタ、１２…ＲＡＭ、１３…アプリケーションプログラムエリア、１４…システムプログラムエリア、１５…異常アクセス信号、４１…システムプログラム、４２…アプリケーションプログラム。

第１図



第２図



特許出願人　日立マクセル株式会社

代理人　弁理士　梶山信是
弁理士　山本富士男